Association for Information Systems
AIS Electronic Library (AISeL)

AMCIS 2002 Proceedings

Americas Conference on Information Systems (AMCIS)

December 2002

A CONCEPTUAL MODEL FOR SECURITY AND TRUST WITHIN INTERNET BANKING TRANSACTIONS

Damien Hutchinson
Deakin University

Matthew Warren
Deakin University

A CONCEPTUAL MODEL FOR SECURITY AND TRUST WITHIN INTERNET BANKING TRANSACTIONS

Damien Hutchinson and Matthew Warren
School of Computing & Mathematics
Deakin University
drh@deakin.edu.au

Abstract

Trust is the foundation upon which E-commerce (EC) is built. The Internet was initially designed for information and resource sharing. The design considerations did not include means for performing electronic transactions. The initiation of transforming business operations on-line in both areas of business to business (B2B) and business to consumer (B2C) commerce translates to the requirement for the secure means of conducting electronic transactions which in the majority of cases will involve the use of Internet banking. Numerous incidences of computer crime have shown the vulnerability of transactions to security threats enforcing the need for the construction of mechanisms to build sustaining trust relationships between business partners and to maintain customer satisfaction between parties conducting EC transactions. This paper deliberates between the issues of EC and business, security of transactions via this medium and the paper offers a conceptual trust model upon which these transactions can be constructed.

Introduction

Trust formed the base upon which traditional commerce was built. E-commerce (EC) does not change this rather it challenges many of the trust assumptions and processes that paper commerce now takes for granted (Keen et al., 2000). The Internet was initially designed for information and resource sharing. The design considerations did not include means for performing electronic transactions. The initiation of transforming business operations on-line in both areas of business to business (B2B) and business to consumer (B2C) EC translates to the requirement for the secure means of conducting electronic transactions, which in the majority of cases will involve the use of Internet banking. Numerous incidences of computer crime have shown the vulnerability of EC transactions to security threats and like the introduction of new information technologies (Mason, 1986; Clarke, 1988) the underlying technologies aimed at securing this open environment are subject to security concerns. The future outlook of EC will be dependant on controlling information security threats, enhancing consumer security perceptions (Friedman et al., 2000; Schneiderman, 2000) and building trust (Hoffman et al., 1999; Keen, 2000). Given the enormous investments to increase security and trust in EC it is essential that mechanisms be designed for trusting this medium. The authors are extensively involved in security research in regards to Internet banking and are currently working with Australian businesses and banks to develop security models for Internet Banking Security. This paper represents an extension of that security research, in developing a trust model to complement the security models that they have developed.

A Definition of Trust

The term trust is defined as the reliance on integrity, justice etc, of a person, or on some quality or attribute of a thing, confidence (Macquarie, 1997). Other definitions include "trust is a term with many meanings" (Williamson, 1993), "trust is itself a term for a clustering of perceptions" (White, 1992), etc, there is not one single definition for the term 'Trust'.

One of the problems in defining what trust is, in a generic manner, is that researchers continue to express concern regarding their collective lack of consensus about trust's meaning (McKnight and Chervany, 1996). To overcome this, researchers at the

University of Minnesota proposed a generic trust model, it defined trust as consisting of the following components (McKnight and Chervany, 1996):

- Trusting Behavior;
- Trusting Intention;
- Situational Decision to Trust;
- Dispositional Trust;
- Trusting Beliefs;
- System Trust;
- Belief Formation Trust.

The development of EC meant that the previous research into trust had to be expanded to take into account new issues, the role of trust within a global market that operates twenty four hours a day. This meant that new trust models had to be developed in order to deal with the complex issues involved in EC.

One of the key aspects in regards to EC is that trust is involved in on-line transactions, users are unsure whether to trust EC because of the anonymous nature of it and the perception of risk that they relate to it (Leitch and Warren, 2000). Other research has shown that many of the risks related to EC relate to the transaction involved. The issues of transactions and trust can be explained by looking at the information available to the parties during an on-line transaction. The three information situations are (Tan and Theon, 2000):

- the situation of perfect information in which all parties know everything that is relevant for a transaction;
- the situation of complete ignorance where none of the parties has information relevant for (a part of) a transaction;
- the intermediary situation of information asymmetry in which one party has information that the other party does not have.

This concept that EC trust was concerned with transactions was formally developed into a generic trust model for EC (as shown by figure 1). The main aspect of the model is that transactional trust is the key area of EC and trust (Tan and Theon, 2000).

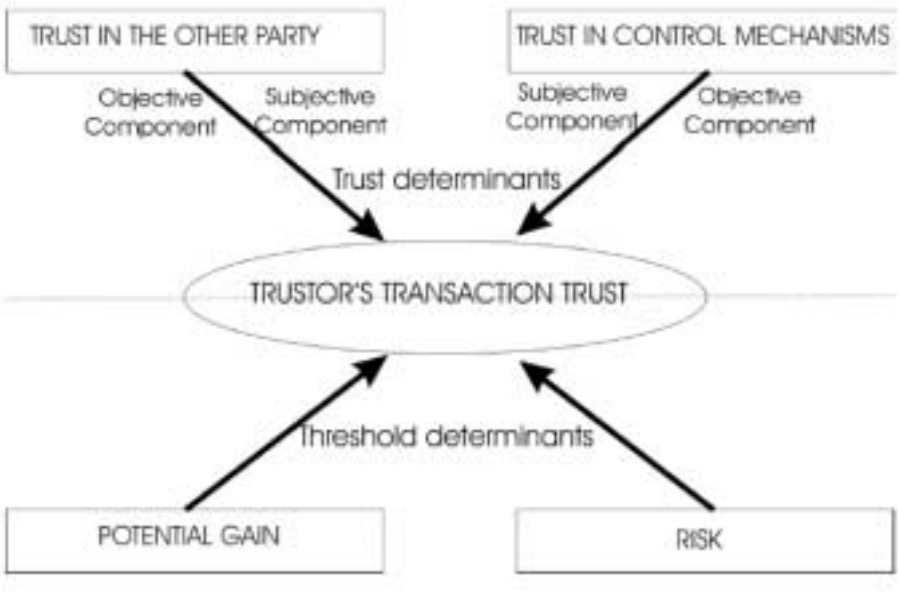

Figure 1. Generic Trust Model for EC (Tan and Theon, 2000)

This generic EC trust model does not help when computer security and trust is considered. Most of the work concerning trust in computer science have been concentrated in the area of security. This is mainly in the form of formal logics to analyze cryptographic protocols for design flaws and correctness (Abdul-Rahman and Hailes, 2000).

As mentioned previously, the authors research focus has predominately been within the research area of computer security. In the area of computer security a trusted system is often intended to be a system that is evaluated against certain well defined criteria like for instance the Trusted Computer System Evaluation Criteria (TCSEC) or Common Criteria (Tjernell, 2000). From this trust becomes a property of a system that can be formally modelled, specified and verified (Denning, 1996). In this setting consumer trust in EC transactions is defined as the subjective probability with which consumers believe that a particular transaction will not occur in a manner consistent with their confident expectations. This maps to the definition of trust where it captures the traditional view of trust in a specific online entity (merchant, bank) and includes trust in the reliability and integrity of the communications medium (Chellappa and Pavlou, 2001).

Another important issue is that perceived information security is the subjective probability with which consumers believe that their personal information will not be viewed, stored, or manipulated during transit or storage by inappropriate parties, in a manner consistent with their confident expectations. For instance, a 128-bit encryption objectively gives the odds of a hacker decrypting a message as one in 2^{128} (Chellappa. and Pavlou, 2002). This does not directly affect the user, but their perception of risk and willingness to use secure services does, therefore the authors decided to develop a security trust model to deal with transactions and related security mechanisms.

Security and Trust in Internet Banking Transactions

When dealing with Internet banking transactions it is imperative that an agreed upon level of trust is maintained throughout the transaction, most probably through mechanisms that guarantee the protection of consumer information in terms of data integrity, confidentiality and privacy which are central to securing the internet banking transaction over the communication network. The failure in any one of these mechanisms at any point within the transaction will result in the security of the transaction being compromised. There have been numerous breaches that have demonstrated such compromise. The motives behind such attacks can be anyone or a combination of the following (Keen et al., 2000):

- Theft or destruction or corruption of valuable data;
- Destruction of network integrity;
- Denial of services;
- Tarnishing of reputation.

Trust has always been a significant factor in influencing customer behaviour towards merchants (Schurr and Ozanne, 1985) and has been demonstrated to be of major importance in uncertain environments like those pertinent to Internet based EC (Fung and Lee, 1999). Security attacks sustained by merchants and Internet retailers from intrusions by hackers not only result in revenue loss and high costs for fixing, maintaining and protecting their systems, but they also project adverse perceptions of transactional security for consumers (Chellappa and Pavlou, 2001). Similarly consumers do not trust Internet marketers sufficiently to engage in "relationship exchanges" involving money and personal information (Hoffman et al. 1999). The trust model for the consumer in traditional commerce is based upon store reputation, brand names and the face-to-face communication that is present in physical interactions (Chellappa and Pavlou, 2001).

In a framework for EC security (Labuschagne, 2000) and a framework of authentication for Internet banking (Hutchinson and Warren, 2001) the elements of authorisation, authentication, integrity, confidentiality and non-repudiation are listed as essential components of securing the EC transaction. The majority of EC transactions are carried out through Web browsers that are connected to merchant sites that in turn connect to some form of financial institution. Like any sound information system the transition when conducting such a transaction should be seamless and transparent for the user but feedback needs to be displayed in order to generate a feeling of control. Some assurance of trust is displayed in browsers and Web sites in the form of symbols for consumers conducting transactions that conform somewhat to these frameworks. Typically an unbroken padlock is used to indicate a secure session facilitating integrity and confidentiality via encryption, statements about data protection and firewalls representing protection, familiar and verifiable domain names for verification and digital certificates ensuring authentication from trusted third parties (Chellappa and Pavlou, 2001).

From a consumer perspective the issue of trust can be ensued by having the following trust elements embedded within the trust model (Chellappa and Pavlou, 2001):

- Protection: This can be defined as the process through which customers are satisfied that their personal information is sufficiently preserved by the entity collecting the information;

- Verification: The inherent lack of implicit identity verification that can be linked with an electronic transaction means that a spurious Web site could easily be created. In relation to Internet banks customers may make the mistake in the domain name, 'www.Citibank.net' instead of 'www.Citibank.com' or may misspell Citibank with a "y" instead of an "i" as in Citybank (Chellappa, 2001);
- Authentication: This is defined as the process through which an Internet merchant can be established via a trusted third party that guarantees that the merchant is indeed who they say they are;
- Non-repudiation: Mechanisms to ensure that client (customer) can be certain it is communicating with the genuine server (Bank) or vice versa, such that neither of the communicating parties can later falsely deny that the transaction took place.

A Conceptual Trust Model for Internet Banking

There have been many approaches and standards released comprising details of managing security by implementing appropriate security technologies. Polices have been written to advise who should have access to what information and procedures of how this information should be obtained. All these approaches work well in theory as a methodology in tackling isolated cases. In practice security needs to be dynamic, adapting to changes that occur in the systems underlying changes to the networks the systems are running on. These approaches to security seem to ignore the premise that security is not a technology rather a process that can only be effectively implemented by properly setting sound boundaries and applying the tools and methods available in a team orientated environment. The transacting parties can repeatedly apply the process aiming to improve and keep the security of their systems up to date. Once the process ceases, security is compromised as new threats and techniques emerge (Wadlow, 2000). Following these principles, this section presents a conceptual trust model incorporating the available security technologies for consumer Internet banking using a process-based approach.

A Transaction Model for Trust with Internet Banking

Many payment systems have been proposed for on-line electronic transactions (O'Mahony et al., 2001). In the majority of these systems the bank plays the role of the payment facilitator. The following outlines the architecture of an EC transaction where the customer is purchasing a product or service from a merchant Web Site with the bank providing the actual exchange of payment. The means of payment is via a credit card. There are essentially two separate transaction models that impact the inherent security mechanisms and origin of trust from the customer point of view. The first model displayed in figure 2 is based on having all the credit card information stored at the bank site and only used when on-line processing takes place.

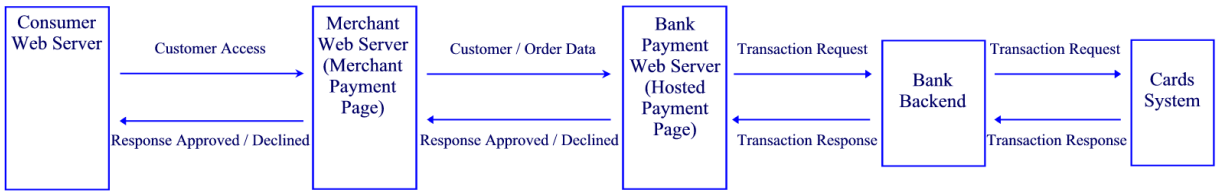

Figure 2. Payment Systems Architecture - Credit Card Information Stored at Bank Site

The second model is where the merchant keeps record of credit card numbers and interaction with the bank occurs in a batch like fashion. This introduces security implications like the need for extensive perimeter and database security, that apart from summing to an option that is both costly and effort intensive specifically for business implementation and maintenance, makes the perception of trust for the customer far more volatile. For the reasons of security and speed of setup, the modelling of security into this transaction process concentrates on the first model, which is based on a hosted payment environment where the credit card information is entered on a payment page that is generated from the bank. The outline of the transaction is displayed in figure 3.

The transaction begins with the customer browsing and selecting a product or service from the merchant Web Site that is handled by the merchant *pre-payment page.* Once the customer has submitted their information for payment the trust model relies on the security implemented between the interactions of the merchant *payment page* and the bank *payment page*. The merchant pre-payment page by passing customer information to the bank payment page initiates these relations. At this stage it is at the merchant's discretion whether the credit card page is presented for the entry of customer information as a separate window or

contained within the merchants environment. The customer information populates predefined fields like the card name and the customer then is able to enter their credit card details. The renowned security implementation of the Secure Socket Layer (SSL) whereby the customer is in a full 128 bit-encrypted environment, hosted from the bank production system, becomes the sole safeguard for securing the session. Once the customer details are entered and are submitted, indicating the desire to proceed with the order, the transaction data is passed to the bank for processing. To complete the transaction process the bank responds by generating a payment receipt for both approval or declined transactions, closes the processing page referring to the page where the customer enters their details and sends a SUCCEED (Approved Transaction) or FAIL (Declined Transaction) URL back to the merchant to enable them to create their own page or pass on these parameters to their own backend systems. From this the only trust that the consumer can believe is based on visual symbols such as the brand of the bank and the closed padlock indicating the security within their session supplied by SSL.

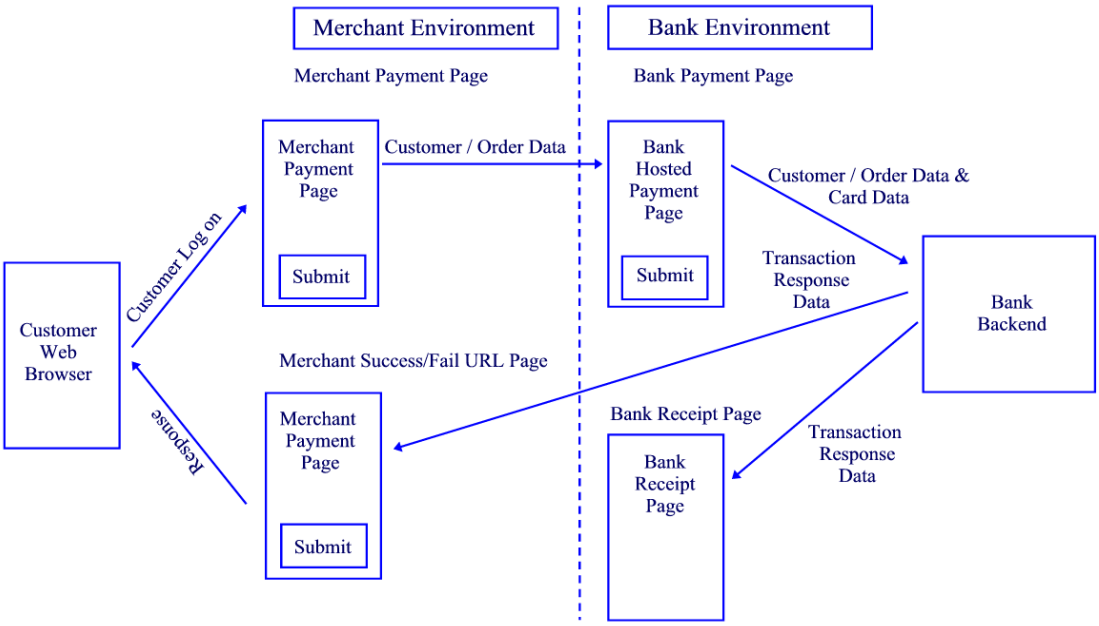

Figure 3. Transaction Process Between the Merchant and Bank Environment

The following is a scenario that illustrates the limited protection that such technologies as SSL can provide (O'Mahony et al., 2001). Suppose an adversary has the objective of obtaining identification numbers (IDs) and passwords from an on-line banking service. This perpetrator has the knowledge that the transmissions between the browser (client) and server (bank) are protected by encryption (SSL). To bypass this technological solution he or she places pamphlets at the banks ATMs encouraging customers to try a new and improved version of the service at www.bank_new_service_site.com (in this example a false domain name). These customers are unaware that the adversary has basically replicated the front page and sign on process of the actual online banking service. When the customer attempts to sign on, the adversary simply captures the IDs and passwords and indicates that the service is not currently available and reroutes the user to the original site. Despite the ability to tamper with customer accounts, the real damage is to the reputations of the customer (which may be the merchant) and bank, which epitomizes a more severe effect than a simple one-time loss of funds. Such scenarios represent the requirement for effective implementation of security and trust in this environment.

A Process Based Model for Trust Within Internet Banking

The illustration of the previous scenario was not to place demise on the effectiveness of current available security technologies but rather to exemplify that in order to create sustained trust the approach to security needs to be one that is based on breaking down and identifying individual components of an electronic transaction and mapping what technologies are available to provide assurance where possible. Significantly although there are means of securing a session between the parties in an electronic transaction (in the case described the customer, the merchant and the bank via SSL) the bigger picture including network

infrastructure whereby millions of parties are interconnected means that breaches as previously demonstrated cannot be dismissed as adversaries can emanate from various internal and external locations. The transaction overview presented in the previous section can be separated into a series of processes that can be defined as separate entities, each requiring a formal security specification and implementation. Based on the transaction identified these processes can be defined as follows:

- The storage (temporary) of the customer information in the merchant pre payment page;
- Merchant passing customer information to the bank payment page;
- Generation of payment receipt; and
- Transmission of approved or declined transaction.

In relation to the use of a credit card for the means of payment in a secure and trusted manner, the following factors must also be considered within this environment (O'Mahony et al., 2001):

- Card validation: ensuring the current card is valid;
- Cardholder Authentication: confirming the cardholder is the genuine cardholder;
- Merchant Authentication: certifying that the merchant is a bona fide member of a payment scheme like Visa or MasterCard; and
- Privacy: endorsing that the details given during the transaction are handled securely and not available to unauthorised parties.

Figure 4 demonstrates a conceptual model of trust in relation to securing the transaction between the consumer, merchant and Internet bank for the purpose of ensuing the required level of confidence for the widespread uptake of EC transactions.

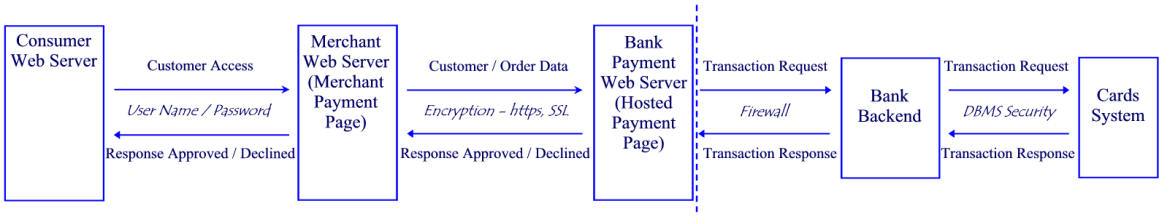

Figure 4. Conceptual Trust Model

This process can be further broken down to show the security implementation at each one of the layers that characterise the EC information transformation for a particular transaction. Figure 5 provides a representation in a hierarchical type structure (Keen et al., 2000) incorporating the integral element of trust.

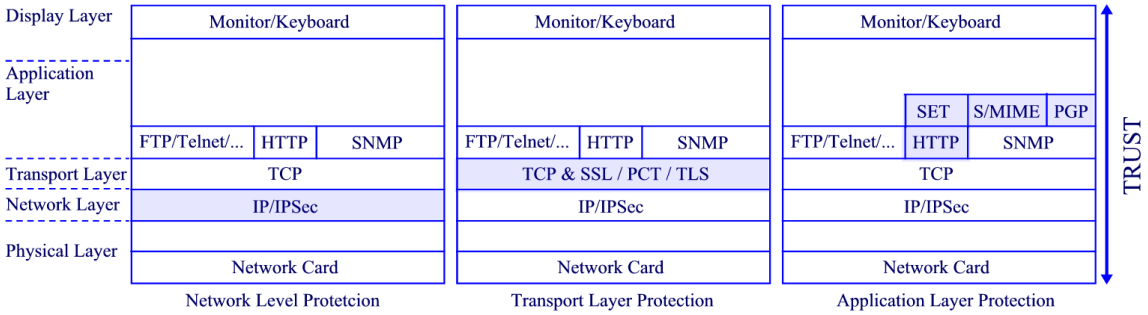

Figure 5. Security Techniques for EC Transaction Transmission Layers

The level of trust that is established in the conceptual model must be maintained from end-to-end in any given transaction. Specifically the trust model employed must be established at the beginning and checks made during the duration of the transaction such that no modification or tampering takes place before the conclusion of the transaction. The technical mechanisms outlined like SSL and other encryption-based methods can act as interim solutions to maintaining this trust. Such technologies though cannot protect against password sniffing or cracking software, spoofing attacks or denial of service attacks. The presentation of

numerous incidents in the past and even more so in recent times has undermined the forte of these technologies especially in relation to Internet banking. Thus there becomes a requirement for some form of authentication procedure. In a networked environment this must be implemented between the client and the server to ensure against non-repudiation, such that the client can be certain it is communicating with the genuine server or vice versa. This could be implemented in the form of a digital signature. Regardless of the technologies that may be used to prevent some of the attacks, the outcome of a successful system infringement remains unchanged. Besides compromising data relating to orders and possible fraudulent activities resulting from copying product information, the most damaging effect would be the adverse publicity (Hutchinson and Warren, 2000) and mending customer confidence especially when businesses are already striving for market share and expansion of their customer base in a very competitive unyielding business world.

Conclusion

EC is bridging the gap for both personal and business use, enabling more convenient transactions (via the Internet) but the associated security threats are real and potentially damaging. Threats pertaining to EC have direct impact on Internet banking security. The vital roles that consumers, merchants and financial institutions play in maintaining the trust bond relies on securing Web clients, the data transaction, the Web server and the underlying network protocol on which the Internet is based. This paper has highlighted the importance of the relationship between security and trust in EC transactions demonstrating that this relationship can be derived from combining the fundamental concepts of EC, made up of the various business issues and the technologies that facilitate the services and applications that define the existence of EC. The case for a new method of formulating such trust was presented in the outline of a conceptual model that employed the idea of processed-based security. Specifically this approach serves the purpose of breaking down the components of an EC transaction to the point where a mapping of security implementations can be viewed as providing trust at the different levels of the transaction process. Critically although the technologies available do provide means via which particular parts of EC transactions can be secured, in the end the ubiquitous uptake of B2B and B2C EC for conducting financial transactions on a large scale will only result from the implementation of an effective model that has both businesses and consumers proclaiming “we can trust this system”.

References

Abdul-Rahman, A. and Hailes, S. (2000) “Supporting Trust in Virtual Communities”, Proceedings of the 33rd Hawaii International Conference on Systems Sciences, Hawaii, USA.

Chellappa, K. (2001) "Contrasting classical electronic infrastructure and the Internet: A tale of caution", Research Paper, Marshall School of business, University of Southern California, Los Angeles, USA.

Chellappa, R. and Pavlou, P. (2001) "Perceived Information Security, Financial Liability and Consumer Trust in Electronic Commerce Transactions", The Marshall School of business, University of Southern California, Los Angeles, USA.

Chellappa, R. and Pavlou, P. (2002) “Perceived Information Security, Financial Liability and Consumer Trust in Electronic Commerce Transactions”, Forthcoming edition of Journal Logistics Information Management, MCB Press.

Clarke, R. A. (1988) "Information technology and dataveillance", Communications of the ACM, Vol. 31 No. 5, pp. 498-512

Denning, D. (1996) "A New Paradigm for Trusted Systems", Proceedings of 1992-1996 ACM SIGSAC New Security Paradigm Workshop, New York, USA.

Fung, R. and Lee, M. (1999) "EC-trust (trust in e-commerce): Exploring the antecedent factors", Proceedings of the 5th Americas Conference on Information Systems, USA.

Friedman, B., Kahn, P. H. and Howe, D. C. (2000) "Trust online", Communications of the ACM, Vol. 43 No. 12, pp. 34-40.

Hutchinson, D. and Warren, M. (2001) "A Framework of Security Authentication for Internet Banking", Proceedings of the Third International Conference on Information Integration and Web-based Applications & Services (IIWAS), September, Linz, Austria.

Hutchinson, W. and Warren, M. J. (2000) "On-line Attacks against Small and Medium sized Enterprises", Proceedings of 1st Australian Information Security Management Workshop, Geelong, Australia.

Hoffman, D. L., Novak, T. P. and Peralta, M. (1999) "Building consumer trust online", Association of Computer Machinery, Communications of the ACM, Vol. 42 No. 4, pp. 80-85.

Leitch, S. and Warren, M.J. (2000) “The role of Ethics in Electronic Commerce”, Proceedings of the 2nd Australian Institute of Computer Ethics Conference, Canberra, Australia.

Labuschagne, L. (2000) "A Framework for Electronic Commerce Security", Phd Thesis, Department of Computer Science, Rand Afrikaans University, South Africa.

Keen, P. (2000) "Ensuring e-trust", Computerworld, March 13, http://www.computerworld.com/cwi/story/0,1199,NAV4774_STO41780,00.html (accessed 19 March 2002).

Keen, P., Ballance, C., Chan, S. and Schrump, S. (2000) Electronic Commerce Relationships: Trust by Design, Prentice-Hall, Inc.

McKnight, D. and Chervany, N. (1996) "The Meaning of Trust", Carlson School of Management Research Paper, University of Minnesota, USA.

Macquarie (1997) The Macquarie Dictionary, The Macquarie Library Pty Ltd, NSW Australia.

Mason, R. O. (1986) "Four ethical issues of the information age", MIS Quarterly, Vol. 10 No. 1, pp. 4-12. http://www.misq.org/archivist/vol/no10/issue1/vol10no1mason.html (accessed 18 March 2002)

O'Mahony, D., Pierce, M. and Tewari, H. (2001) Electronic Payment Systems for E-Commerce, Artech House, London.

Schneiderman, B. (2000) "Designing trust into online experiences", Communications of the ACM, Vol. 43 No. 12, pp. 34-40.

Schurr, P. H. and Ozanne, J. L. (1985) "Influences on exchange processes: Buyers' preconceptions of a seller's trustworthiness and bargaining toughness", Journal of Consumer Research, Vol. 11 No. 4, pp. 939-953.

Tan, Y. and Thoen, W. (2000) "Formal Aspects of a Generic Model of Trust for Electronic Conference", Proceedings of the 33rd Hawaii International Conference on Systems Sciences, Hawaii, USA.

Tjernell, L. (2000) "A Study of Users' Trust in e-Commerce", MSc Thesis in Computer and systems sciences, Stockholm University, Sweden.

Wadlow, T. A. (2000) The Process of Network Security, Addison-Wesley Longman Inc. USA.

White, H. (1985) "Agency as control". In J. W. Pratt & R. J. Zeckhauser (Eds.), Principals and agents: The structure of business: 187-212. Boston: Harvard Business School Press.

Williamson, O. E. (1993). "Calculativeness, trust, and economic organization". Journal of Law and Economics, 34: 453-502.